Multimedia Tools and Applications (2020) 79:30557–30581
https://doi.org/10.1007/s11042-020-09499-w

DCT-based color digital image blind watermarking method with variable steps

Zihan Yuan[1] · Decheng Liu[1] · Xueting Zhang[1] · Huanying Wang[1] · Qingtang Su[1]

Received: 23 September 2019 / Revised: 23 June 2020 / Accepted: 29 July 2020 /
Published online: 15 August 2020

Abstract
In this paper, a blind watermarking method for color digital image based on DCT domain with variable steps is proposed to solve the copyright protection of color digital image. In this method, partial DCT coefficients of the image block transformed by two-dimensional discrete cosine transform (2D-DCT) are selected in the transform domain firstly, then these selected DCT coefficients at different positions are quantized by different quantization steps, and the embedding and blind extraction of digital watermark are completed. This method used color digital image as watermark image instead of gray image or binary image, and the color host image used in this scheme is selected from two public image databases (CVG-UGR and USC-SIPI). The experimental result shows that this scheme embedded color digital image watermark into host image successfully not merely has high invisibility, but also has strong robustness, which is suitable for digital image copyright protection.

Keywords Blind watermarking · Color image · Discrete cosine transform · Variable steps

1 Introduction

Because of the growing popularity of the Internet, the communication of multimedia information has reached unprecedented depth and breadth, we can publish our works and get the information we need through the Internet [13, 14, 25, 27, 32] easily by using computer or smartphone [10]. At the same time, digital products, especially color digital images, have been widely spread on the Internet. However, a series of serious problems have arisen, such as piracy, infringement, tampering and so on. Therefore, how to make full use of the Internet and protect copyright effectively has been paid more and more attention. As a new subject of information security, information hiding science [40] has generated. The information hiding

✉ Qingtang Su
sdytsqt@163.com

[1] School of Information and Electrical Engineering, Ludong University, Yantai 264025, China

technology hides secret information in carrier files [22] in order to prevent secret information from being discovered, modified, stolen and damaged by some ulterior persons, so as to achieve the purpose of copyright protection [3, 23, 31] and insure the information transmission security on the Internet. As an important branch of information hiding science, digital watermarking method [2, 6, 35–37] has achieved great development in recent years, and has become an effective digital product copyright protection and data security maintenance technology. The successful embedding and extraction of digital watermark can solve the problem of copyright protection effectively.

According to different classification criteria, watermarking schemes are divided into different types. For example, according to the extraction method of digital watermark, the digital watermarking scheme can be divided into blind watermarking algorithm [35–37] and non-blind watermarking algorithm [29, 30]. Among them, blind watermarking algorithm requires no participation of original data and original watermark in the process of watermark extraction. On the contrary, the non-blind watermarking algorithm requires the participation of the original data or the original watermark when extracting the watermark. Therefore, compared with non-blind watermarking algorithm, blind watermarking algorithm has higher security and robustness, and has higher practical value and broader application prospect.

In addition, according to different processing methods of host image, digital watermarking algorithm is divided into spatial domain watermarking algorithm [1, 39] and transform domain watermarking algorithm [33–37]. Spatial domain watermarking algorithm is to directly modify the pixel value on the original data to embed the watermark bit information. For example, Su et al. [39] proposed a blind watermarking algorithm which is based on approximate Schur decomposition in spatial domain. This method calculates the approximate greatest eigenvalue of Schur decomposition firstly, and then uses the obtained approximate greatest eigenvalue to accomplish the embedding and extraction process of color digital watermark image. In this method, all of the operations are performed in the spatial domain, which does not require the real Schur decomposition and has extremely high real-time performance. Transform domain watermarking algorithm is more complex than that of spatial domain. It is a reversible digital transformation of the original data information before embedding the digital data. According to certain rules, some coefficients of the transformation domain are modified to embed the digital watermark, and then the data embedded in the watermark is reconstructed by using the inverse transformation to achieve the extraction of the watermark. Discrete Cosine Transform (DCT) [4, 38], [19–21] Discrete Wavelet Transform (DWT) [7, 18, 29], [8, 15, 26] and Discrete Fourier Transform (DFT) [28] all belong to the transform domain watermarking method. The transform domain watermarking algorithm can conveniently integrate some features of the human visual system (HVS) into the watermarking algorithm, which has a strong ability to resist malicious attacks and signal processing. Compared with spatial watermarking algorithm, it has better robustness, so at present the research of watermarking algorithm mainly focuses on the transform domain watermarking algorithm.

For example, Jane et al. [7] proposed a hybrid non-blind watermarking algorithm based on DWT and singular value decomposition (SVD), which has strong robustness and can resist various attacks. But this method needs the original data to extract the watermark, which belongs to the non-blind watermarking algorithm. However, compared with non-blind watermarking algorithm, blind watermarking algorithm has more practical value and application prospect. Ernawan et al. [4] proposed a robust image watermarking method based on optimal DCT psychological threshold. In this method, the selected host image pixel blocks are transformed by DCT, and the DCT coefficients at specific locations are modified by certain rules to embed the watermark, and gray image is used as host image and binary image is used as watermark image. Using two-level DCT, Su et al. [38] proposed a color digital watermark image embedding algorithm. This method can carry out copyright protection and resist many common attacks effectively, but the algorithm uses DCT operations two times, so it has a long embedding and extraction time, high computational complexity. Thus, its real-time performance is poor. Leng et al. [20, 21] proposed two methods for face and palmprint recognition in DCT domain, and the characteristics of DCT coefficients at different location and the method how to select and weight coefficients were analyzed. What's more, making full use of the advantages of DCT, Leng et al. [19] proposed a dual-source discrimination power analysis for multi-instance contactless palmprint recognition, which has good performance.

A RGB blind watermarking algorithm using SVD is proposed by Golea et al. [5]. The watermark images used in this method are RGB color image, and the extraction does not need the original image, which is a blind watermarking algorithm. In addition, Su et al. [37] proposed a blind color image watermarking scheme based on QR decomposition. In this method, the color image watermark is embedded into the element in the first row and fourth column of matrix *R,* the matrix *R* is gained by QR decomposition, and this algorithm has strong robustness.

A good digital watermarking technology requires the embedded watermark not only has high invisibility but also has strong robustness. Therefore, how to design a digital watermarking algorithm with high invisibility and strong robustness simultaneously has become a research hotspot.

Taking advantage of the strong robustness of frequency domain digital watermarking algorithm, in this paper, a blind color digital image watermarking method based on variable steps and 2D-DCT is proposed. It's worth noting that this proposed method is not belong to reversible watermarking method, thus it is not belong to the reversible data hiding [16, 17]. In the proposed method, the color host image and the color watermark image are divided into R, G and B three color components firstly, and the color components are divided into fixed size image blocks. Then, selecting part of DCT coefficients of host image blocks after 2D-DCT based on zig-zag order, the DCT coefficients at different positions are quantized by different quantization steps, and the embedding and blind extraction of digital watermark are completed. This method has the advantageous of high invisibility, strong robustness and high real-time performance, which meets the requirements of copyright protection for color digital images.

Other parts of this paper are structured as follows. The second part is the theoretical basis, which include Arnold transform, Pseudo random selection algorithm, and 2D-DCT. The specific processes of watermarking method are presented in the third part. The fourth part gives the simulation outputs and analysis, and finally the fifth part gives the conclusion.

2 Preliminaries

2.1 Arnold transform

Arnold transform is a kind of commonly used image scrambling technology, it can be regarded as a tensile, compression, folding and stitching process. Through this process, the points in the discrete digital image matrix can be rearranged. Arnold scrambling transform is often used in front of the other image processing for image preprocessing, such as scrambling digital blind watermark before embedding it. And, Arnold transform can also be used for normal image encryption. Scrambling the digital watermark firstly and then hiding it could improve the security of watermark and the robustness of the algorithm. Therefore, Arnold transform is widely applied in the watermark image scrambling. This transformation realizes encryption by replacing the pixel point in the original image with the coordinate of (*x*, *y*) to the position. Encryption is achieved by moving the pixel value from the original point (*x*, *y*) to the new point (*x*', *y*'). The image after Arnold transform becomes chaotic and its matrix operation formula is as follow:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{mod P} \tag{1}$$

where *x*, *y*, *x*', *y*' are four integers in{0, 1, 2,…, *P*-1}, mod(.) is the modulo function, *P* is the edge length of the image matrix, and (*x*', *y*') is the coordinates of the pixel (*x*, *y*) after the Arnold transform.

When Arnold transform is used to scramble the original image, the scrambling times can be used as the private key, so as to enhance the confidentiality and security of the system and achieve the purpose of information hiding. The scrambled image can be easily restored through the Arnold inverse transform. The inverse process of Arnold transformation is shown in Eq. (2).

$$\begin{bmatrix} x \\ y \end{bmatrix} = \left(\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} + \begin{bmatrix} P \\ P \end{bmatrix} \right) \bmod P \tag{2}$$

2.2 Pseudo random selection algorithm

In random replacement algorithm, improper replacement strategy without any modification of random sequences is easy to repeat the selected pixel bits repeated several times, resulting in a pixel can be embedded multiple information, and the after embedded information can destroy the first embedded information. In order to avoid collision and enhance the security of watermarking method, in this paper, a pseudo random selection algorithm based on the private key *KB* is used to select nonoverlapping embedded blocks randomly. The formula is given as follows:

$$R = \text{ceil}\left(\text{rand}\left(1, \sqrt{HT}\right) / \sqrt{ST}\right) \tag{3}$$

$$C = \begin{Bmatrix} KB \times k + 1 & \mathit{if}\ \text{mod}(R, 2) = 1 \\ KB \times (k + 1) & \mathit{else} \end{Bmatrix} \tag{4}$$

where, *HT* denotes the number of the nonoverlapping image blocks of size 8 × 8, *ST* denotes the embedded blocks number, *R* and *C* represent the row number and column number of selected blocks in the host image, ceil(.) is a function that round up to an integer, rand(.) is a random number generation function, mod(.) is the modulo function, and $k = 0, 1, 2, ..., \sqrt{ST} - 1$.

2.3 2D-DCT

DCT is a kind of transform which is parallel to DFT, while DCT is based on the orthogonal transformation of real numbers, so the DCT is a special case of the Fourier transform. DCT is a signal decomposition as well as compression technology, which is extensively applied in the aspect of digital signal processing. DCT is widely used in many standards of image coding and compression, so it is implemented in many occasions easily [19]. In addition, DCT algorithm has the advantages of fast operation speed, high precision and easy implementation in digital signal processor, so it plays an important role in image processing.

DCT is a common method in transform domain. The transform results include a direct current (DC) coefficient and some alternate current (AC) coefficients. The DC coefficient represents the average brightness, and the AC coefficients concentrate the main energy of the original image block. Generally speaking, the process of embedding watermark in DCT domain is actually the process of adding watermark information to DCT coefficients, and then obtaining watermarked image through inverse DCT transform.

2D-DCT means to perform DCT again based on the one-dimensional DCT. The 2D-DCT is defined by Eq. (5):

$$F(u,v) = c(u)c(v) \times \left[\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \cos\frac{(2x+1)u\pi}{2M}\cos\frac{(2y+1)v\pi}{2N}\right] \tag{5}$$

where,

$$c(u) = \left\{\begin{array}{cc} \sqrt{1/M} & u=0 \\ \sqrt{2/M} & u=1,2,\ldots,M{-}1 \end{array}\right\}$$
$$c(v) = \left\{\begin{array}{cc} \sqrt{1/N} & v=0 \\ 2/N & v=1,2,\ldots,N{-}1 \end{array}\right\}$$

x and y are the sampling values in the spatial domain, $f(x, y)$ is the pixel value at coordinates (x, y) in the spatial domain, u and v are the sampling values in the frequency domain, $F(u, v)$ is the frequency coefficient at coordinates (u, v) after 2D-DCT in the frequency domain, M and N are the size of the row and column of matrix A. In digital image processing, the digital image is usually represented by square matrix of pixels, that is $M = N$.

The formula of inverse transform of 2D-DCT (2D-IDCT) is defined as follows:

$$f(x,y) = c(u)c(v) \times \left[\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v) \times \cos\frac{(2x+1)u\pi}{2M}\cos\frac{(2y+1)v\pi}{2N}\right] \tag{6}$$

2.4 Selection of embedding location

In this paper, the first four DCT coefficients of each image block which belong to low-frequency coefficients are used to embedding the watermark. As we all know, when the low-frequency coefficients are used to embed the watermark information, the watermarking method will be more robust, while the medium frequency coefficients can balance the robustness and imperceptibility when they are used to embedding the watermark. As a matter of fact, this proposed method mainly considers improving the robustness of the watermarking method, so we selected the first four DCT coefficients to complete the watermark embedding and extraction. Regarding the balance between robustness and invisibility, this paper adopts quantization step to solve it.

In addition, the selection on the first four DCT coefficients in low-frequency coefficients not only meets the JPEG standard, but also ensures the compaction of the energy, which means the proposed method can resist the attack of JPEG compression better [38].

3 The proposed method

The implementation of the watermarking method includes three steps: quantization steps selection, watermark embedding and watermark extraction. As shown in Fig. 1, the main steps of the watermarking method are given as follows:

3.1 Selecting quantization steps

The specific steps of the quantization steps selection are described as follows:

Step 1: Preprocessing the host image, dividing each of the selected standard host images which size is $M \times M$ (Lena, F16, Peppers, House, Baboon, Bear, Barbara, Couple, Kid, Sailboat) into nonoverlapping pixel blocks of size $P \times P$, and then DCT was performed on each pixel block.

Step 2: For improving the security of watermarking method, the MD5 hash pseudo random selection algorithm based on private key Kb_i is used to choose the pixel blocks randomly. Then, in order to obtain the size relations between first four DCT coefficients of pixel blocks

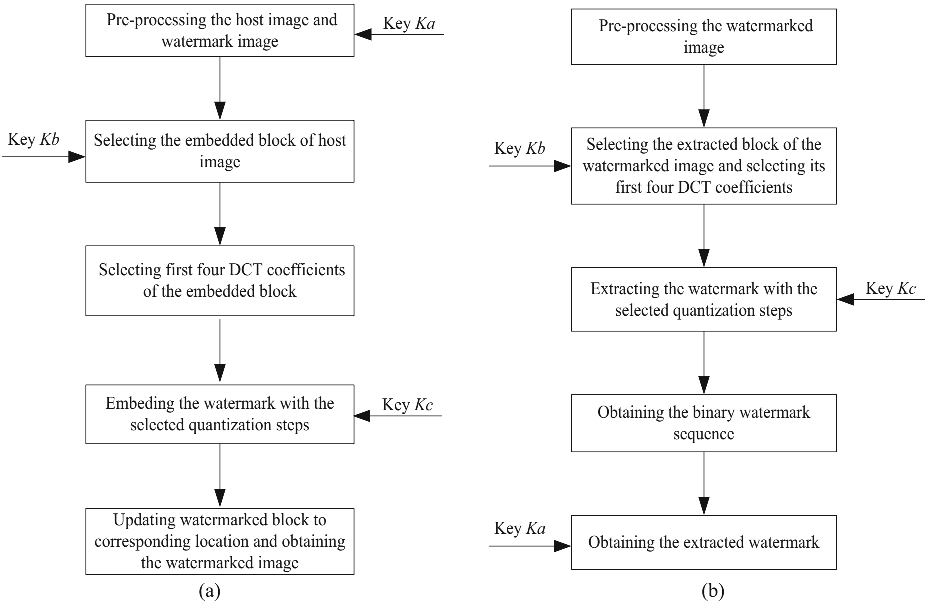
Pre-processing the host image and watermark image
Key Ka
Key Kb
Selecting the embedded block of host image
Selecting first four DCT coefficients of the embedded block
Embeding the watermark with the selected quantization steps
Key Kc
Updating watermarked block to corresponding location and obtaining the watermarked image
(a)
Pre-processing the watermarked image
Key Kb
Selecting the extracted block of the watermarked image and selecting its first four DCT coefficients
Extracting the watermark with the selected quantization steps
Key Kc
Obtaining the binary watermark sequence
Key Ka
Obtaining the extracted watermark
(b)

Fig. 1 The watermarking algorithm flow chart: (**a**) watermark embedding process. (**b**) watermark extraction process

which selected according to the zig-zag order, namely the DC coefficient and the first three AC coefficients, the regression analysis is conducted on the four DCT coefficients. According to this relationship, four different quantization steps T_j can be obtained, where $j = 1, 2, 3, 4$. The relationships between the four different quantization steps T_j are:

$$T_1 = 13.70 \times T_4 \tag{7}$$

$$T_2 = 0.81 \times T_4 \tag{8}$$

$$T_3 = 1.61 \times T_4 \tag{9}$$

where, T_1 is the quantization step of DC coefficient, T_2, T_3 and T_4 are the quantization steps of the first three AC coefficients respectively. The key step T_4 can be obtained according to experimental data.

Step 3: Making the quantization steps as key Kc_j and used them in the process of watermark embedding and watermark extraction.

3.2 Embedding watermark

The specific description of watermark embedding is given by the steps below:

Step 1: A color host image H with size of $M \times M$ is divided into three layered host images H_i of red, green and blue by dimension reduction processing, and then each layered host image H_i is divided into nonoverlapping pixel blocks with size of $P \times P$, where $i = 1, 2, 3$ represents each color layer of host image in RGB color model.

Step 2: A color digital watermark image W of size $N \times N$ is divided into three layered watermark images W_i of red, green and blue, and conducting Arnold transform with the private key Ka_i to improve the watermark security. Converting each decimal pixel value of the layered watermark image W_i into 8-bit binary number, and connecting the binary information successively to obtain sequence SW_i with a length of $8N^2$, where $i = 1, 2, 3$ represents each color layer of watermark image in RGB color model.

Step 3: In order to improve the security of watermarking method, the MD5 hash pseudo random selection algorithm based on private key Kb_i is used to choose the pixel block randomly, where $i = 1, 2, 3$ represents each color layer of host image in RGB color model.

Step 4: According to Eq. (10), 2D-DCT is performed on the selected pixel block A to obtain the transformation matrix $dctA$, and the first four DCT coefficients c_j of the transformation matrix $dctA$ are selected according to the zig-zag order, where $j = 1, 2, 3, 4$.

$$dctA = \mathrm{dct2}(A) \tag{10}$$

where dct2 (.) is the 2D-DCT function.

Step 5: Selecting 4 watermark bits w_j from the watermark sequence SW_i successively. By using Eqs. (11) and (12), the four DCT coefficients c_j are quantized by the corresponding quantization step T_j based on private key Kc_j, in order to get the upper boundary number $Chigh_j$ and lower boundary number $Clow_j$ of each DCT coefficient.

$$Chigh_j = \left\{ \begin{array}{ll} \mathrm{abs}\left(c_j\right) - \mathrm{mod}\left(\mathrm{abs}\left(c_j\right), T_j\right) + 1.25 \times T_j, & \mathit{if}\ w_j =' 0' \\ \mathrm{abs}\left(c_j\right) - \mathrm{mod}\left(\mathrm{abs}\left(c_y\right), T_j\right) + 0.75 \times T_j, & \mathit{if}\ w_j =' 1' \end{array} \right\} \tag{11}$$

$$Clow_j = \left\{ \begin{array}{ll} \mathrm{abs}\left(c_j\right) - \mathrm{mod}\left(\mathrm{abs}\left(c_j\right), T_j\right) + 0.25 \times T_j, & \mathit{if}\ w_j =' 0' \\ \mathrm{abs}\left(c_j\right) - \mathrm{mod}\left(\mathrm{abs}\left(c_j\right), T_j\right) - 0.25 \times T_y, & \mathit{if}\ w_j =' 1' \end{array} \right\} \tag{12}$$

where, w_j is the j-th watermark bit to be embedded, abs(.) is the absolute value function, mod(.) is the modulo function, and T_j is the j-th quantization step, $j = 1, 2, 3, 4$.

Step 6: Using Eq. (13) to compute the best boundary number CC_j, and replacing the original DCT coefficient of corresponding position of transformation matrix *dctA* with CC_j to get the watermarked transformation matrix $dctA^*$.

$$CC_j = \left\{ \begin{array}{ll} Clow_j \times \mathrm{sign}\left(c_j\right), & \mathit{if}\ \mathrm{abs}\left(Clow_j - \mathrm{abs}\left(c_j\right)\right) \le \mathrm{abs}\left(Chigh_j - \mathrm{abs}\left(c_j\right)\right) \\ Chigh_j \times \mathrm{sign}\left(c_j\right), & \mathit{else} \end{array} \right. \tag{13}$$

where sign (.) is sign function, abs(.) is absolute value function, $j = 1, 2, 3, 4$.

Step 7: According to Eq. (14), 2D-IDCT is performed on the transformation matrix $dctA^*$ to obtain the watermarked pixel block A^*, and then the watermarked pixel block is updated to its corresponding position in the layered host image H_i, where $i = 1, 2, 3$ represents each color layer of host image in RGB color model.

$$A^* = \mathrm{idct2}\left(dctA^*\right) \tag{14}$$

where idct2 (.) is the inverse 2D-DCT function.

Step 8: Steps 3–7 of this process is repeated to ensure all watermark bit has been embedded. Thus, watermarked layered image H_i^* is obtained. Finally, the watermarked image H^* is obtained by combining the three watermarked layered images H_i^*, where $i = 1, 2, 3$ represents each color layer of watermarked image in RGB color model.

3.3 Extracting watermark

The specific description of watermark extracting is shown by the steps below:

Step 1: Dividing watermarked image H^* into three layered images which is red, green and blue layer respectively. Meanwhile, dividing each watermarked layered image H_i^* into nonoverlapping pixel blocks of size $P \times P$, where $i = 1, 2, 3$ represents each color layer of watermarked image in RGB color model.

Step 2: For improving the security of watermarking method, the MD5 hash pseudo random selection algorithm based on private key Kb_i is used to choose the watermarked pixel blocks A^* from watermarked layered image H_i^*, where $i = 1, 2, 3$ represents each color layer of watermarked image in RGB color model.

Step 3: 2D-DCT is carried out on the selected watermarked pixel block A^* to obtain the transformation matrix $dctA^*$, and four DCT coefficients c_j^* corresponding to the embedding process in the transformation matrix $dctA^*$ are selected according to the zig-zag order, where $j = 1, 2, 3, 4$ respectively represent the j-th DCT coefficient.

Step 4: Using the corresponding quantization step T_j based on private key Kc_j to extract the watermark bit W_j^* from the watermarked pixel block A^* according to Eq. (15).

$$w_j^* = \begin{cases} '1', & if \bmod\left(\mathrm{abs}\left(c_{\mathrm{j}}^*\right), T_j\right) < 0.5 \times T_j \\ '0', & else \end{cases} \tag{15}$$

where mod(.) is the modulo function, abs(.) is absolute value function, and T_j is the j-th quantization step, $j = 1, 2, 3, 4$.

Step 5: Repeating Step 2 to Step 4 of this process to extract and obtain the binary watermark sequence SW_i^* of each layer. Then dividing each 8-bits binary information in the watermark sequence SW_i^* into a group, and converting it into decimal pixel value. Then combining decimal pixel values to form a chaotic layered watermark image, where $i = 1, 2, 3$ represents each color layer of extracted watermark image in RGB color model.

Step 6: Performing inverse Arnold transform based on private key Ka_i for each layered watermark image to obtain the extracted watermark image of each layer W_i^*. At the same time, the extracted watermark images of each layer W_i^* are combined to form the final extracted watermark image W^*, where $i = 1, 2, 3$ represents each color layer of extracted watermark image in RGB color model.

4 Experimental results

For testing performance of the presented algorithm, ten color digital images of size 512 × 512 which are shown in Figs. 2(a)-(j) are used as host images in the following experiments. All of the host images we used are standard color images selected from databases CVG-UGR [41] and USC-SIPI [42]. The watermark images include two simple color digital images of size 32 × 32, which are given in Fig. 3(a)-(b). What's more, in order to prove the universality of the proposed method, we also selected a real natural color image "Leopard" of sized 32 × 32 as the watermark image for the relevant comparison test. After embedding watermark, a series of simulation attacks are carried out. In order to evaluate the performance of the algorithm more accurately and objectively, the experimental results are compared with some relevant color image watermarking methods. Such as a robust watermarking algorithm based on chaotic system and QR decomposition [33], a color digital watermark image embedding algorithm based on two-level DCT [38], bind RGB watermarking algorithm which is using SVD [5], a blind color digital image watermarking method using QR decomposition [37], a new fast and robust image watermarking method in spatial domain for color image [36], and a blind image watermarking scheme using 2D-DCT [43].

In the following experiments, we used some commonly used and widely recognized indicators to evaluate the quality of watermarked images. Specifically, peak signal to noise ratio (PSNR) and structural similarity index measurement (SSIM) are used to evaluate the invisibility of digital watermark. Normalized cross-correlation (NC) is used to evaluate the robustness of digital watermarking method. PSNR is the most common and widely used objective evaluation index of image quality, it computes the similar degree of original host

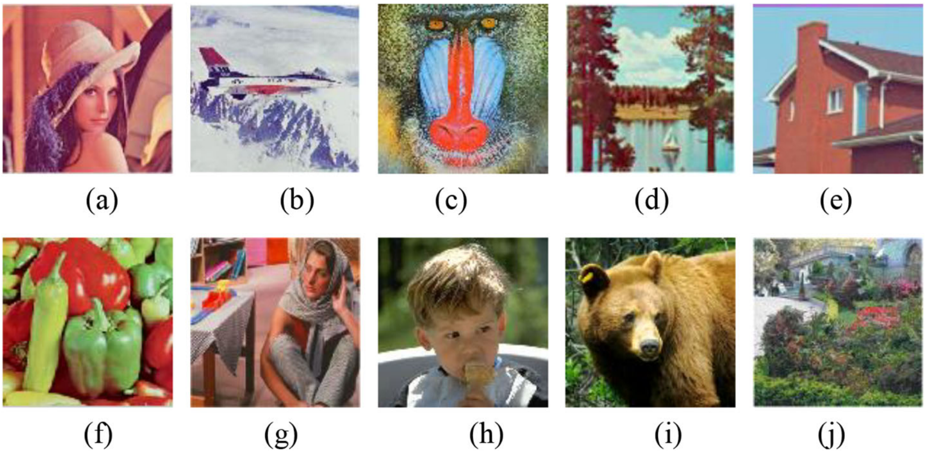

Fig. 2 Host images: (**a**) Lena (**b**) F16 (**c**) Baboon (**d**) SailBoat (**e**) House (**f**) Peppers (**g**) Barbara (**h**) Kid (**i**) Bear (**j**) TTU

image H and watermarked image H^*, so that evaluating the invisibility of watermark. The unit of PSNR is dB. Generally speaking, a higher PSNR value means less distortion and better image quality. PSNR of color digital image named MPSNR (M-layer PSNR) is defined as follows:

$$MPSNR = 20\lg \frac{2^d - 1}{\sqrt{\frac{1}{N_1 \times N_1 \times M} \sum_{x=1}^{N_1} \sum_{y=1}^{N_2} \sum_{j=1}^{M} \left[H(x, y, j) - H^*(x, y, j) \right]^2}} \tag{16}$$

in which, $H(x,y,j)$ is the pixel point which location is (x, y) of the host image in layer j; similarly, $H^*(x,y,j)$ is the pixel point which location is (x, y) of watermarked image in layer j; N_1 and N_2 are the size of row and column of the used image respectively; as for 24-bit color image, each layer is an 8-bit image ($d = 8$).

SSIM is a measure of similarity between two pictures. According to the characteristics of human vision, human vision can easily extract structural information from images. Therefore,

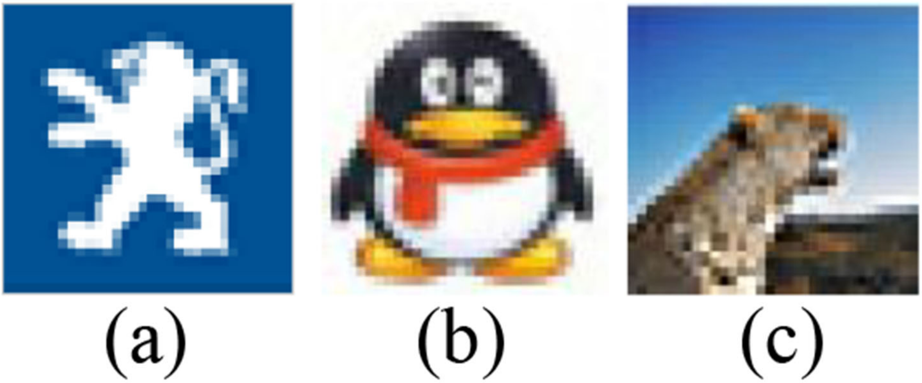

Fig. 3 Watermark images: (**a**) Logo (**b**) QQ (**c**) Leopard

calculating the similarity of the structure information of two images can be used to detect the quality of images. The value of SSIM is greater than 0 and less than 1. The higher the value is, the smaller difference of watermarked image and original image is, in other words, quality of image is better. When the two images are identical, the value of SSIM is 1.

The definition of SSIM is as follows:

$$SSIM\left(H,H^{*}\right)=l\left(H,H^{*}\right)c\left(H,H^{*}\right)s\left(H,H^{*}\right) \tag{17}$$

in which,

$$\begin{cases} l\left(H,H^{*}\right)=\left(2\mu_{H}\mu_{H^{*}}+C_{1}\right)/\left(\mu_{H}^{2}+\mu_{H^{*}}^{2}+C_{1}\right) \\ c\left(H,H^{*}\right)=\left(2\sigma_{H}\sigma_{H^{*}}+C_{2}\right)/\left(\sigma_{H}^{2}+\sigma_{H^{*}}^{2}+C_{2}\right) \\ s\left(H,H^{*}\right)=\left(\sigma_{HH^{*}}+C_{3}\right)/\left(\sigma_{H}\sigma_{H^{*}}+C_{3}\right) \end{cases} \tag{18}$$

l(H,H)* is a function that using for luminance comparison, μ_H and μ_H represent average values of image *H* and *H** respectively, and is used to compare the similarity of the average brightness of the two images. *c(H,H*)* is a function that using for contrast comparison, σ_H and σ_{H^*} represent standard deviation of the images *H* and *H** respectively, it is used to compare the similarity of contrast between two images. *s(H,H*)* is a function that using for structural comparison, σ_{HH^*} represents the covariance of *x* and *y,* which is used to evaluate correlation coefficient of two digital images.

What's more, normalized cross-correlation (NC) is an effective evaluation criterion for watermarking algorithm robustness. NC does not contain any subjective factors, so it is relatively fair and reliable. The value of NC is greater than 0 and less than 1. The value of NC is larger, the watermarking method is more robust, and the quality of image is better. As for color digital image watermarking algorithm, the calculation of NC is defined as follows:

$$\mathrm{NC}=\frac{\sum\limits_{j=1}^{3}\sum\limits_{x=1}^{m}\sum\limits_{y=1}^{n}\left(W(x,y,j)\times W^{*}(x,y,j)\right)}{\sqrt{\sum\limits_{j=1}^{3}\sum\limits_{x=1}^{m}\sum\limits_{y=1}^{n}[W(x,\mathrm{y},j)]^{2}}\sqrt{\sum\limits_{j=1}^{3}\sum\limits_{x=1}^{m}\sum\limits_{y=1}^{n}\left[W^{*}(x,y,j)\right]^{2}}} \tag{19}$$

where, *W* and *W** represent the original color image digital watermark and the extracted color image digital one, respectively. And, *m* and *n* represent the row size and column size of the color image digital watermark respectively, $1 \le x \le m$, $1 \le y \le n$, *j* represents the number of layers of color image digital watermark.

4.1 The selection of block size and quantization step

As we all know, the block size could affect the performance of watermarking method to a certain extent. Considering the invisibility, robustness and capacity, we have conducted a series of experiments to select an appropriate block size *P*. Since this scheme takes advantage of the first four DCT coefficients to complete the watermark embedding, thus its block size *P* should be greater than or equal to 4. In addition, if the block size *P* is greater than 16, the watermark cannot be embedded completely. Thus, taking the host image "Lena" in Fig. 2 (a) and the watermark image "Logo" in Fig. 3 (a) as an example, we compared the performance of this watermarking method with block size of 4 × 4, 8 × 8, and 12 × 12, respectively. The experimental results are shown in Table 1. Considering the balance of the performances of watermarking algorithm, the block size *P* is chosen as 8 in this paper.

In addition, it is well known that quantization step is an important parameter in watermarking algorithm. And we need to do some preparatory work before choosing the quantization step reasonably. Due to the different sizes of DCT coefficients, we decide to use different quantization steps to quantify different DCT coefficients. This is what we were mentioned in the third section of this paper.

Therefore, we only need to select the quantization step T_4 for further getting the quantization steps T_1, T_2 and T_3 according to their relations. In order to select a reasonable quantization step, the color digital watermark images are embedded into the color host images by using different quantization steps. Figure 4 shows the values of SSIM under different quantization steps and the average value of NC under different attacks. Figure 4 shows that, when the value of T_4 is increasing, the SSIM value gets smaller and smaller, the average NC value gets bigger and bigger, which indicates that with the increase of the quantization step T_4, the invisibility of watermark gets worse and worse, while the robustness of watermark gets better and better. In order to keep the balance of both robustness and invisibility of the proposed watermarking method, quantization step T_4 could be chosen from 10 to 17. In this paper, we choose a quantization step T_4 to be 10. Correspondingly, the value of T_1 is 13.7, the value of T_2 is 8.1, and the value of T_3 is 16.1, respectively.

4.2 The imperceptibility test and analysis

Imperceptibility also named invisibility, on the one hand, it requires that the embedded watermark must not cause significant distortion of the carrier image; on the other hand, it requires the embedded watermark information is not invisible in subjective. Invisibility is an important index to measure the performance of watermarking algorithm. To evaluate the invisibility of the watermark, the watermarks in Figs. 3(a) and (b) are embedded into the host image in Figs. 2(a)-(j) respectively. Table 2 shows the PSNR value and SSIM value of the extracted watermark image. Table 2 shows that, after embedding "Logo" and "QQ" in Fig. 3 into ten different host images, almost of the PSNR values are more than 35 *dB*, and the average SSIM value is close to 1. This means that the watermark is imperceptible through human visual system after embedding, and the proposed watermarking method satisfies the requirement of imperceptibility of watermarking technology.

In addition, the watermark image "Logo" in Fig. 3(a) is embedded to the host image "Lena" in Fig. 2(a) and host image "F16" in Fig. 2(b) respectively, and the watermark image "QQ" in Fig. 3(b) is embedded to the host image "Sailboat" in Fig. 2(c) and host image "House" in Fig. 2(d) respectively, so as to evaluate invisibility of our watermarking algorithm further. Then, we compared the invisibility between different schemes. Table 3 shows PSNR and SSIM values of different methods after embedding two watermarks into different color host images respectively. Table 4 shows the average NC value of the extracted watermark without attack after embedding different watermarks into different color host images with different methods. It is worth noting that since the scheme [38] proposed by Su et al. is a two-level DCT

Table 1 The performance of watermarking method with different block sizes without attack (PSNR/SSIM/NC)

Block size	PSNR	SSIM	NC
4 × 4	35.9635	0.9412	1.0000
8 × 8	36.3689	0.9616	1.0000
12 × 12	36.2929	0.9709	0.9693

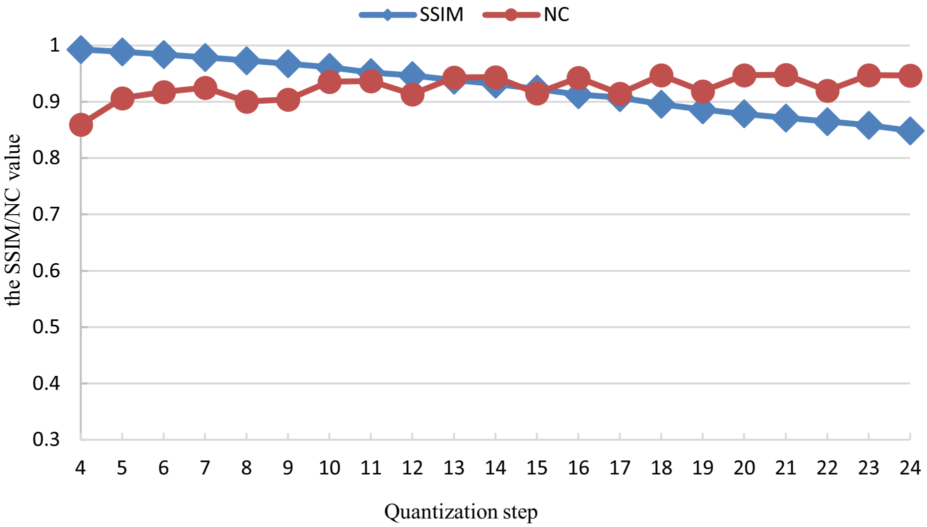

Fig. 4 The SSIM value and average NC value in various quantization steps

watermarking algorithm, while the proposed scheme is a one-level DCT method, the one-level DCT part of the selected scheme [38] is used to compare with the watermarking method in this paper.

As can be seen from Table 3, in scheme [33], the value of PSNR and SSIM are very low, which indicate scheme [33] has poor watermark invisibility. The scheme [38] has high PSNR and SSIM, that is, it had excellent watermark invisibility. However, it can be seen from Table 4 that its NC value is relatively small so the watermark robustness is poor. PSNR values of schemes [5, 36, 37, 43] are not much different from those of the proposed scheme, while their SSIM values are less than those of the presented method. The average PSNR value is more than 36 *dB*, and the average SSIM value is near to 1 in the presented method, which indicating that the invisibility of the proposed scheme is better. In addition, it can be seen from Table 4 that, when there is no attack, the NC values of the proposed scheme are 1, and the NC values of method [5, 33, 37, 38] are less than 1. It shows that the proposed scheme has a good balance between invisibility and robustness, and it can meet the requirements of both invisibility and

Table 2 The results of invisibility of watermark images embedded in host images (PSNR/SSIM)

	Logo	QQ
Lena	36.3689/0.9616	36.3462/0.9606
F16	36.3257/0.9562	36.2951/0.9562
Baboon	35.6565/0.9845	35.8645/0.9854
Sailboat	35.6829/0.9589	35.7044/0.9579
House	35.7442/0.9447	35.9358/0.9471
Peppers	35.5343/0.9382	35.5588/0.9386
Barbara	35.8316/0.9621	35.7279/0.9607
Kid	34.8236/0.9454	34.6188/0.9434
Bear	34.5134/0.9216	34.3918/0.9173
TTU	35.4818/0.9775	35.6121/0.9775
Average	35.5963/0.9551	35.6056/0.9545

Table 3 The invisibility comparative results of different methods (PSNR/SSIM)

Host image	Method [33]	Method [38]	Method [5]	Method [37]	Method [36]	Method [43]	Proposed method
Lena	22.5616/0.6332	48.6761/0.9956	38.0535/0.9414	36.3777/0.9140	38.0535/0.9413	37.5851/0.9350	36.3689/0.9616
F16	23.2864/0.7111	40.7425/0.9708	39.4358/0.9656	36.4075/0.9064	38.1039/0.9353	37.1426/0.9245	36.3257/0.9562
Baboon	22.3026/0.6846	41.6958/0.9857	31.4794/0.9613	36.3953/0.9698	37.8455/0.9787	36.0501/0.9720	35.8645/0.9854
Sailboat	18.7103/0.6301	45.7757/0.9933	35.5318/0.9094	36.3855/0.9161	37.6796/0.9440	38.4131/0.9412	35.7044/0.9579
Average	21.7152/0.6648	44.2225/0.9864	36.1251/0.9444	36.3915/0.9266	37.9206/0.9498	37.2978/0.9432	36.0659/0.9653

Table 4 The comparison of NC value of different methods

Host image	Method [33]	Method [38]	Method [5]	Method [37]	Method [36]	Method [43]	Proposed method
Lena	1.0000	0.9475	0.9937	1.0000	1.0000	1.0000	1.0000
F16	0.9975	0.8568	0.9949	1.0000	1.0000	1.0000	1.0000
Baboon	1.0000	0.8441	0.9976	1.0000	1.0000	1.0000	1.0000
Sailboat	1.0000	0.8746	0.9806	0.9999	1.0000	1.0000	1.0000
Average	0.9994	0.8808	0.9917	1.0000	1.0000	1.0000	1.0000

robustness. Therefore, compared to these relevant methods, the method we presented in this paper has good performance.

4.3 The robustness test and analysis

Robustness is also known as hardiness, it refers to the capacities of watermarked image that can still retain watermark information after being modified intentionally or unintentionally. The robustness of watermarking is also one of the important characteristics of watermarking method.

To evaluate the robustness of the proposed watermarking scheme, we embedded the watermark image “Logo”, “QQ”, and “Leopard” in Fig. 3 into the host image “Lena”, “pepper”, and “F16” in Fig. 2 respectively. And then a series of attacks are carried out on watermarked images, such as compression attack, noise addition, filter attack, resize attack, and crop attack. The results of experiments are described in Figs. 5, 6 and 7. As we all know, in the process of image transmission, the image is often compressed or attacked by noise [11, 12, 24], and making image quality degradation and data loss [9]. A robust watermarking method requires that the watermark image extracted after the attacks still has a good visual effect. Beside display visual effects of the extracted watermark image after attacks, we used NC value to evaluate robustness of this watermarking method. As an objective standard to measure the similarity between the extracted watermark W^* and the original watermark W, the value of NC can effectively evaluate the robustness of the watermarking method.

After watermark image “Logo” in Fig. 3(a) is embedded into host image “Lena” in Fig. 2(a), we carried out a series of attacks and compared the robustness with other related methods [5, 37, 38], [36, 43] to prove robustness of this watermarking algorithm further. We do not compare the robustness with method [33], because its PSNR values and SSIM values are too low in the previous invisibility comparison, which means its invisibility is too poor. Therefore, for the sake of fairness, method [33] is not used as a comparison in the analysis of algorithm robustness. The comparison results of NC values of different schemes after attacks are shown in Figs. 8, 9, 10, 11, 12, 13, 14 and 15.

JPEG compression is a popular compression method, and JPEG compression attack is an effective attack method to verify the robustness of watermarking algorithm. In the experiments, we used a compression factor from 10 to 100 with increment 10 for image compression. Figure 8 shows the experimental results of watermarked images after JPEG compression attacks with compression factors of 50 and 90 respectively.

Similarly, JPEG2000 compression attack is an effective attack method to verify the robustness of watermarking algorithm. It was developed by JPEG in order to improve the performance of JPEG compression attack. Similar to JPEG compression, in the JPEG 2000

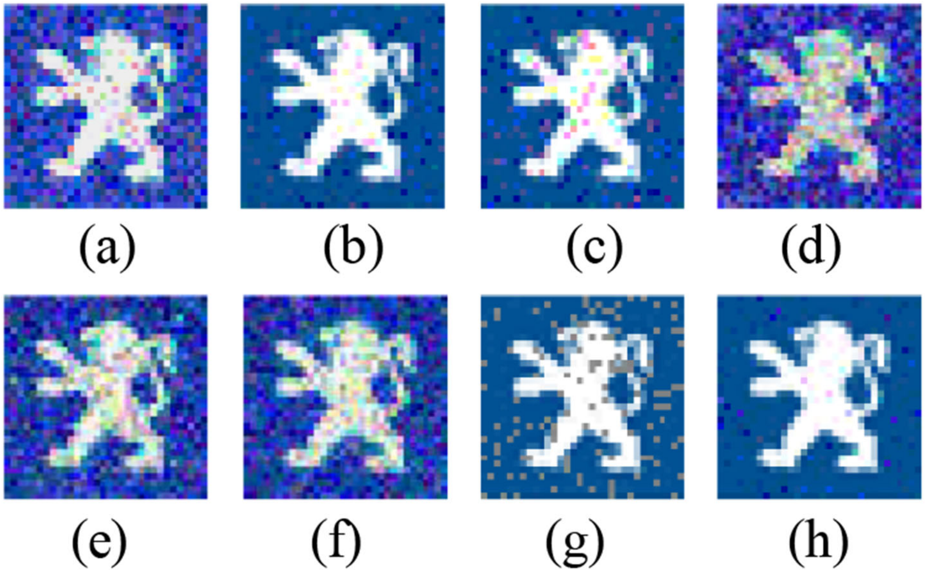

Fig. 5 The robustness experimental results under various attacks: (**a**) JPEG (quality factor = 50) NC = 0.9891 (**b**) JPEG 2000 (compression ratio = 4:1) NC = 0.9889 (**c**) Salt &Peppers noise (noise intensity = 0.2%) NC = 0.9841 (**d**) Gaussian white noise (variance = 0.001) NC = 0.8763 (**e**) Median filtering (filter window = 3 × 3) NC = 0.9134 (**f**) Butterworth low-pass filtering (filter order = 5) NC = 0.8648 (**g**) Cropping (cropping ratio = 12.5%) NC = 0.9664 and (**h**) Zoom-in (enlarging ratio = 4:1) NC = 0.9941

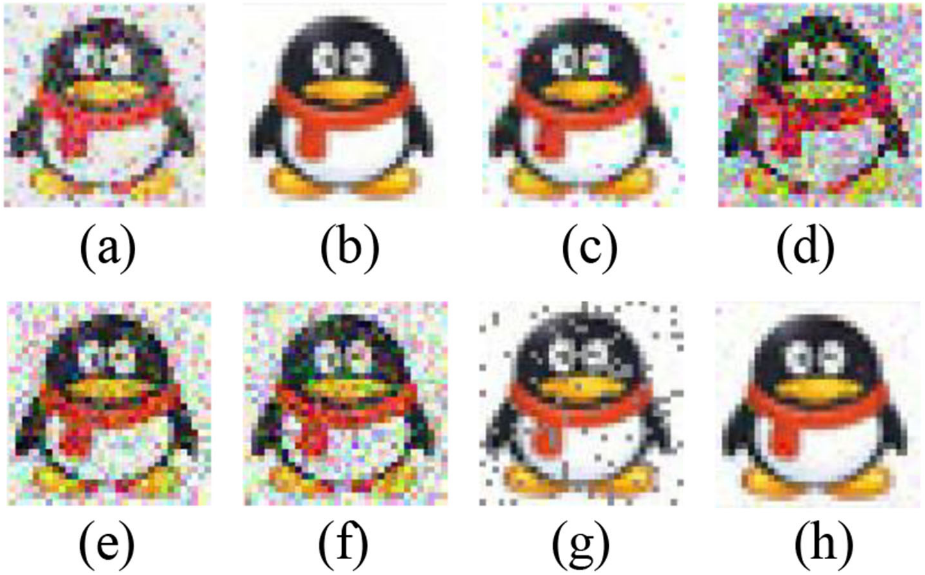

Fig. 6 The robustness experimental results under various attacks: (**a**) JPEG (quality factor = 50) NC = 0.9349 (**b**) JPEG 2000 (compression ratio = 4:1) NC = 0.9996 (**c**) Salt &Peppers noise (noise intensity = 0.2%) NC = 0.9806 (**d**) Gaussian white noise (variance = 0, 0.001) NC = 0.7958 (**e**) Median filtering (filter window = 3 × 3) NC = 0.8858 (**f**) Butterworth low-pass filtering (filter order = 5) NC = 0.8880 (**g**) Cropping (cropping ratio = 12.5%) NC = 0.9615 and (**h**) Zoom-in (enlarging ratio = 4:1) NC = 0.9932

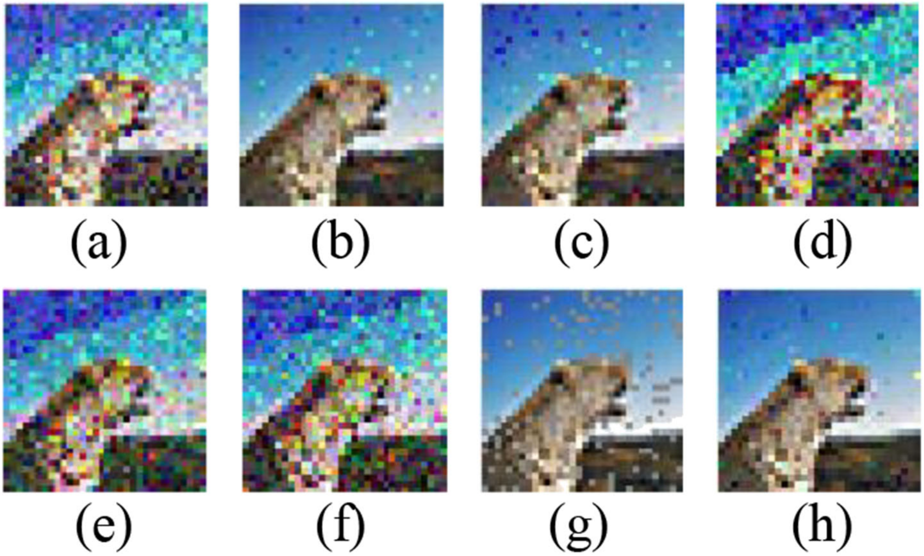

Fig. 7 The robustness experimental results under various attacks: (**a**) JPEG (quality factor = 50) NC = 0.9737 (**b**) JPEG 2000 (compression ratio = 4:1) NC = 0.9950 (**c**) Salt &Peppers noise (noise intensity = 0.2%) NC = 0.9960 (**d**) Gaussian white noise (variance = 0.001) NC = 0.9378 (**e**) Median filtering (filter window = 3 × 3) NC = 0.9512 (**f**) Butterworth low-pass filtering (filter order = 5) NC = 0.9298 (**g**) Cropping (cropping ratio = 12.5%) NC = 0.9850 and (**h**) Zoom-in (enlarging ratio = 4:1) NC = 0.9957

compression attack experiment, we use a compression factor from 1 to 10 with increment 1 for image compression. Figure 9 shows the experimental results of watermarked images after compression attacks by JPEG 2000 with compression factors of 5 and 10 respectively. From Figs. 8 and 9, we can see that compared with other watermark schemes, the proposed scheme has good robustness for different image compression attacks.

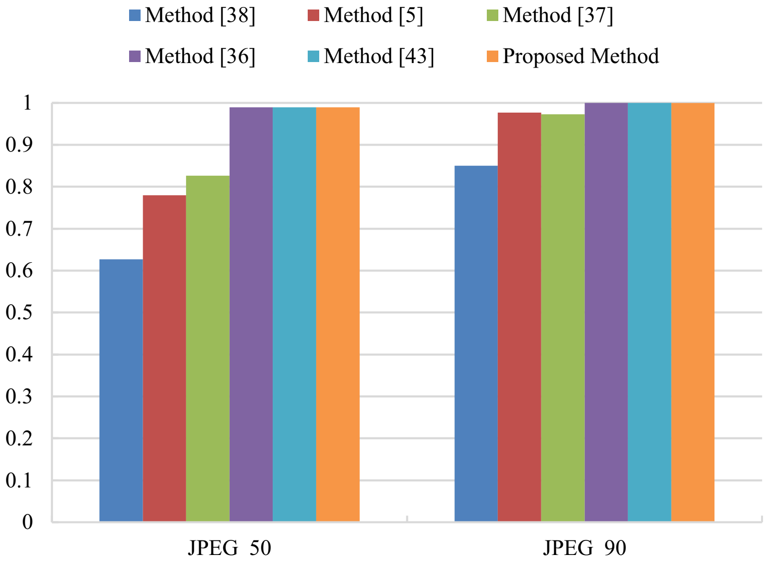

Fig. 8 The robustness comparative results when watermarked image attacked by JPEG compression

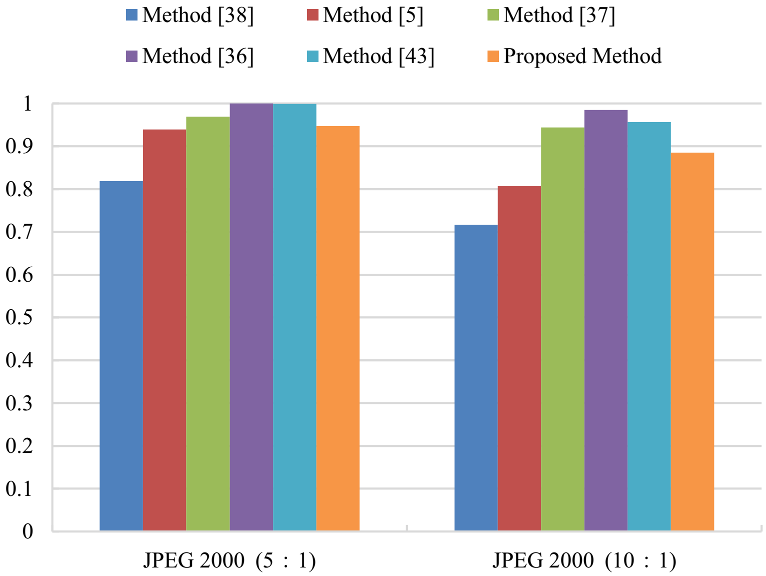

Fig. 9 The robustness comparative results when watermarked image attacked by JPEG2000 compression

Figure 10 shows the NC values of watermarks that extracted from watermarked images after Salt & Peppers noising attacks with noise intensity of 0.2% and 1% respectively. It can be seen that the proposed scheme is more robust to resist Salt & Peppers noising attack than other related schemes. Figure 11 gives the experimental results that watermarked images after Gaussian noise attacks with the mean value is 0, variances are 0.001 and 0.003, respectively. It can be seen that although all methods show low robustness to Gaussian noise attacks, the watermarking scheme proposed by us is relatively better in general.

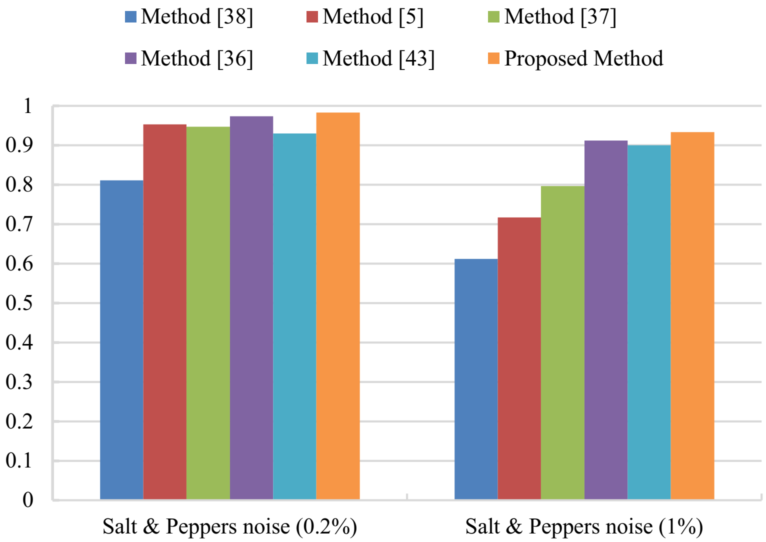

Fig. 10 The robustness comparative results when watermarked image attacked by Salt &Peppers noise

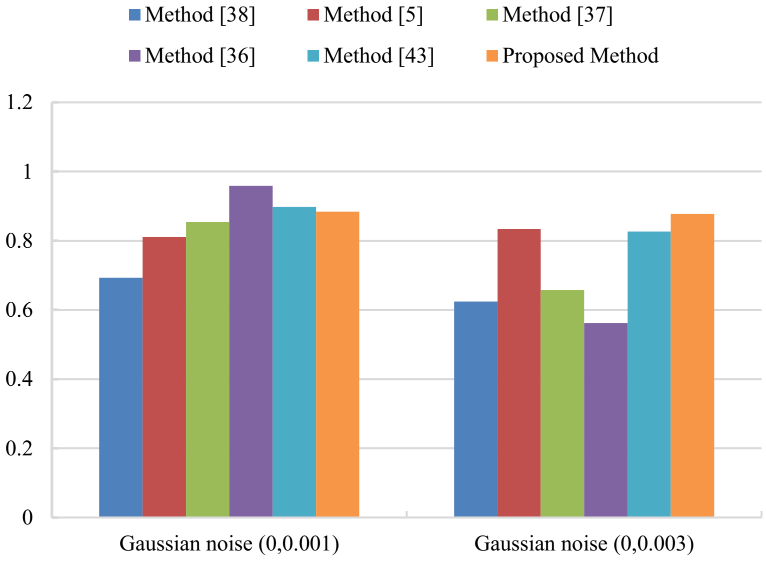

Fig. 11 The robustness comparative results when watermarked image attacked by Gaussian noise

Figure 12 gives experimental results of watermarked image attacked by the median filtering of different sizes. Median filtering attacks with filter windows of 2 × 2 and 3 × 3 are carried out on the watermarked images respectively. Figure 13 shows the results of watermarked image attacked by the Butterworth low-pass filtering which filter orders of 3 and 5 respectively. Figures 12 and 13 show that the proposed scheme has strong robustness for resisting different filtering attacks.

Figure 14 gives the experimental results after enlarging watermarked image by 400% and shrinking it by 50% respectively. It can be seen that the listed algorithms generally have good

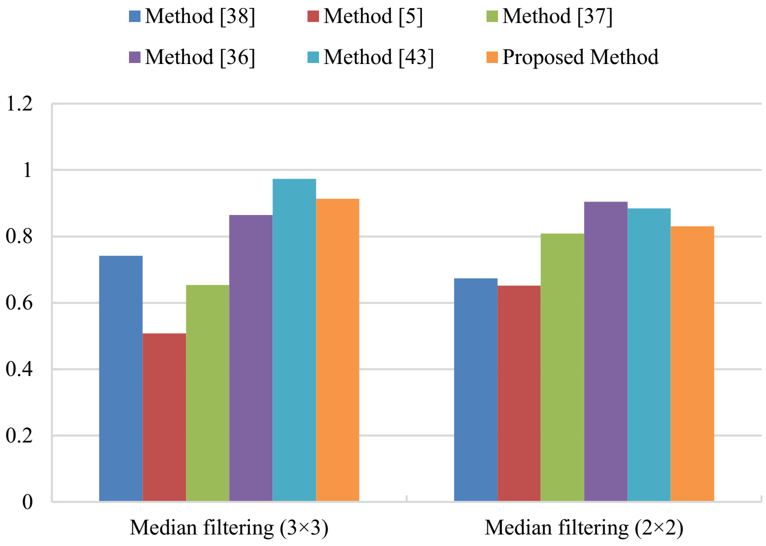

Fig. 12 The robustness comparative results when watermarked image attacked by Median filtering

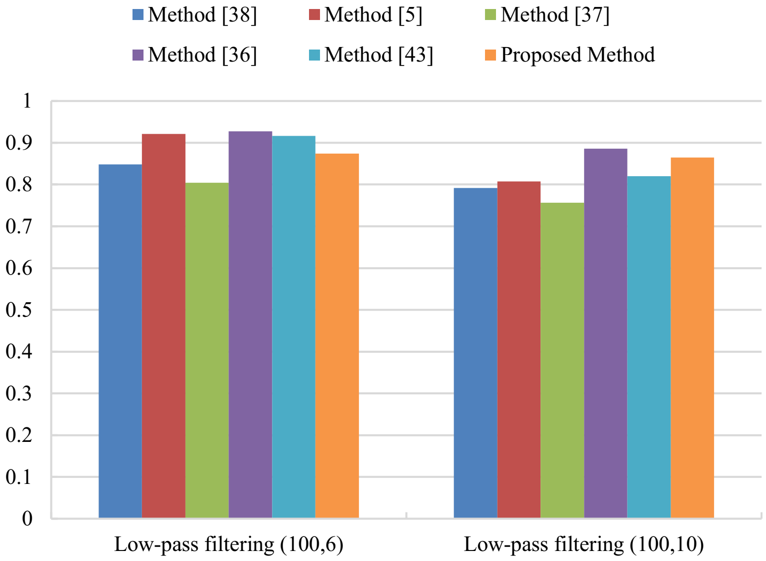

Fig. 13 The robustness comparative results when watermarked image attacked by Butterworth low-pass filtering

robustness to zooming in attack and relatively poor robustness to zooming out attack. It is because that the rows and columns of the image are lost regularly when the image is attacked by zooming out.

Image cropping is a common method in image processing. Figure 15 gives the results that watermarked image after cropping attacks which cropping ratio of 25% and 50%. It is indicated that the presented watermarking algorithm can resist cropping attack.

To evaluate the robustness more accurately, in Table 5, the comparison of average values of NC between various algorithms after different attacks which are given in Figs. 8, 9, 10, 11, 12,

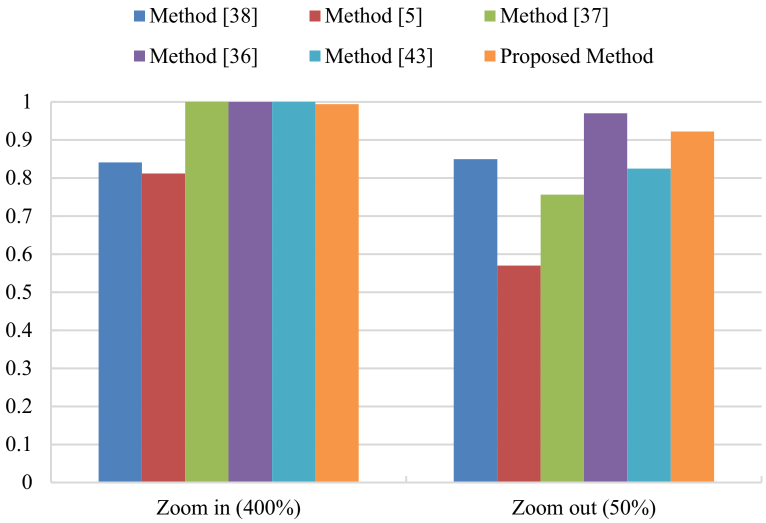

Fig. 14 The robustness comparative results when watermarked image attacked by scaling attacks

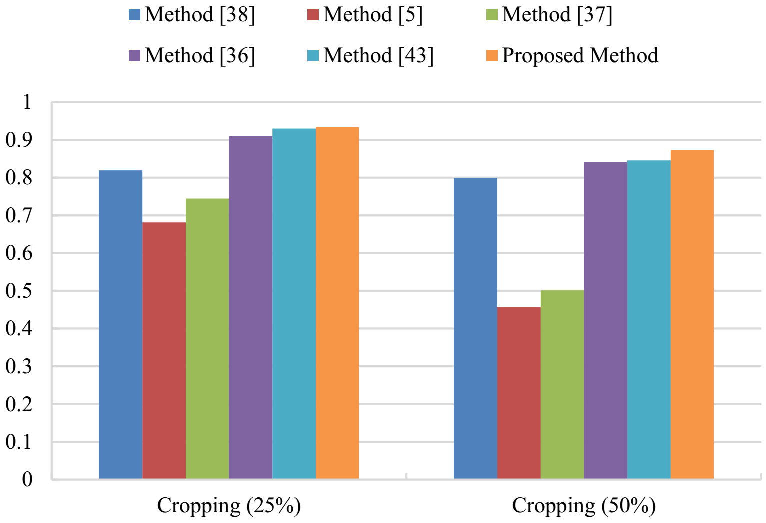

Fig. 15 The robustness comparative results when watermarked image attacked by cropping attacks

13, 14 and 15. From Table 5, it can be seen that the average NC value of our proposed scheme is 0.918419, which is higher than other schemes. Therefore, the robustness of this scheme is better than that of schemes [5, 37, 38], [36, 43].

4.4 The embedding capacity analysis

Generally speaking, as for watermarking algorithm, embedding capacity could be calculated through embedded watermark bits number and host image pixel number. The embedding capacity is also an important factor to measure the quality of watermarking algorithm. Table 5 shows the embedding capacity comparison results of the presented watermarking algorithm and other related algorithms. As is shown in Table 6, as for method [38], its embedding capacity is higher compared with other methods. This is because the method [38] embedded one bit of watermark information in the DC coefficient and seven bits of watermark information in the AC coefficients, and used watermark image with size of 64 × 64. The embedding capacity of our algorithm is equal to that of methods [5, 36, 37, 43]. Because the five methods are embedding 24-bit watermark images of size 32 × 32 to a color digital host image with size of 512 × 512, so their embedding capacity is $(32 \times 32 \times 24)/(512 \times 512 \times 3) = 0.03125$(Bit/Pixel).

Table 5 The average NC of different methods after various attacks

Method	Average NC
Method [38]	0.757300
Method [5]	0.764000
Method [37]	0.812119
Method [36]	0.917631
Method [43]	0.917938
Proposed method	0.918419

Table 6 The embedding capacity of various watermarking methods

Watermarking method	Watermark Length (Bit)	Host image (Pixel)	Bit/Pixel
Method [38]	64 × 64 × 24	512 × 512 × 3	0.12500
Method [5]	32 × 32 × 24	512 × 512 × 3	0.03125
Method [37]	32 × 32 × 24	512 × 512 × 3	0.03125
Method [36]	32 × 32 × 24	512 × 512 × 3	0.03125
Method [43]	32 × 32 × 24	512 × 512 × 3	0.03125
Proposed method	32 × 32 × 24	512 × 512 × 3	0.03125

4.5 The real-time feature analysis

All of the algorithms in this paper are run on platform 2.60GHZ CPU, 4.00GB RAM, Win10, MATLAB (R2017a). Table 7 compares the embedding time and extraction time of the proposed algorithm with those of other related methods to measure the real-time feature of our proposed method. As we can see from Table 7, the running time of our proposed method is much less than that of method [38], slightly less than that of method [5, 43], not much different from that of method [37]. The running time of method [36] is less than other methods, it is because that this method is a spatial-domain watermarking method, which computational complexity is low, while other mentioned methods are belong to transform-domain watermarking method that has high computational complexity. In the proposed method, the average embedding time is 1.503906 s, and average extracting time is 0.484375 s, thus total time is 1.988281 s, which can better meet the real-time requirements of the watermarking algorithm.

4.6 The security analysis

A good digital watermarking scheme not only needs to meet the requirements of invisibility, robustness, watermark capacity, real-time feature, but also need good security. Therefore, for improving the security of the proposed method, color watermark image is preprocessed firstly in this paper. The 24-bit color watermark image is divided into three layered watermark images: red, green and blue. Then, applying Arnold transform with private key Ka_i to each layered watermark image. The private key Ka_i is determine by the integer memory type, we know that the range of integers is between 1 and 32,768, so the space of each private key Ka_i is 2^{15}. Because the color watermark image has three layers of red, green and blue, thus the key space of Arnold transform is 2^{45}.

Table 7 The running time comparison of various methods (Second)

Watermarking method	Watermark embedding time	Watermark extraction time	Total time
Method [38]	3.437500	61.125000	64.562500
Method [5]	1.909066	0.905951	2.815017
Method [37]	0.686992	0.427006	1.113998
Method [36]	0.383260	0.340666	0.723926
Method [43]	3.031250	0.718750	3.750000
Proposed method	1.503906	0.484375	1.988281

Table 8 The security comparison of different schemes

Method	Key space
Method [38]	2^{45}
Method [5]	2^{30}
Method [37]	2^{126}
Method [36]	2^{126}
Method [43]	2^{225}
Proposed method	2^{189}

In addition, the original host image is divided to red, green, blue layers while the host image is preprocessed. Then each layered host image is segmented to blocks, and using MD5 hash pseudo random selection algorithm based on the private key Kb_i to choose the embedded blocks randomly. The private key Kb_i is decided by the size of original host image, the size of embedded block, and key space in MD5. Therefore the key spaces of them are 2^9, 2^3 and 2^{16}, respectively. Thus the key space of private key Kb_i is the product of each key space, that is 2^{28}. Similarly, since the color host image has three layers of red, green and blue, the key space is 2^{84}.

What's more, the private key Kc_j is used to complete the watermark embedding and extraction where $j = 1, 2, 3, 4$, which also improves the security of this proposed method. The private key Kc_j is determine by the integer memory type, so the space of each private key Kc_j is 2^{15}, and the total key space of private key Kc_j is 2^{60}.

In conclusion, key space of the proposed watermarking method is 2^{189}. As we all know, watermarking methods with a key space of more than 2^{112} are enough secure for current applications. Thus our proposed method has high security. Table 8 gives the key spaces of different related watermarking methods. As can be seen from Table 8, the key space of the proposed method is much larger than the key space of methods [5, 36–38] but slightly smaller than method [43].

5 Conclusion

In this paper, a blind image watermarking method based on 2D-DCT with variable steps is proposed to protect the copyright of color image. At first, partial DCT coefficients of specific locations are selected; then, different quantization steps are adopted to quantify different DCT coefficients according to the relationship between the selected coefficients that we found; at last, the embedding and blind extraction of color watermark are completed. The advantages of the presented method include the following three points: 1) the relationship between the first four DCT coefficients is analyzed and obtained in this paper; 2) variable quantization steps are adopted to improve the invisibility and robustness of the watermarking method; 3) this method uses color image instead of gray image or binary image as host image and watermark image which is different to most watermarking schemes. Experimental results show that this method can meet the requirements of invisibility, robustness, real-time and security of watermarking scheme, and it is suitable for the copyright protection of digital color image.

Acknowledgements This work was supported by the National Natural Science Foundations of China (No. 61771231, 61772253, 61572258, and 61602229), and the Key Research and Development Program of Shandong Province (No. 2019GGX101025, 2019GGX101032).

References

1. Abraham J, Paul V (2019) An imperceptible spatial domain color image watermarking scheme. Journal of King Saud University-Computer and Information Sciences 31(1):125–133
2. Botta M, Cavagnino D, Pomponiu V (2016). A modular framework for color image watermarking. Elsevier North-Holland, Inc, 119 102–114
3. Cedillo-Hernandez A, Cedillo-Hernandez M, Miyatake MN, Meana HP (2018) A spatiotemporal saliency-modulated JND profile applied to video watermarking. J Vis Commun Image Represent 52:106–117
4. Ernawan F, Kabir MN (2018) A robust image watermarking technique with an optimal dct-psychovisual threshold. IEEE Access 6(4):20464–20480
5. Golea NEH, Seghir R, Benzid R (2010). A bind RGB color image watermarking based on singular value decomposition, in: IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), 1–5.
6. Huynh-The T, Hua CH, Tu NA, Hur T, Bang J, Kim D, Amin MB, Ho Kang B, Seung H, Lee S (2018) Selective bit embedding scheme for robust blind color image watermarking. Inf Sci 426:1–18
7. Jane O, Elbaşi E, İlk HG (2014) Hybrid non-blind watermarking based on DWT and SVD. Journal of Applied Research & Technology 12(4):750–761
8. Jindal H, Kasana SS, Saxena S (2016). A novel image zooming technique using wavelet coefficients. in Book: Proceedings of International Conference on Recent Cognizance in Wireless Communication and Image Processing, 1–7, Springer, New Delhi, India. [ISBN: 978-81-322-2638-3]
9. Jindal H, Kasana SS, Saxena S (2018) Underwater Pipelines Panoramic Image Transmission and Refinement using Acoustic Sensors. International Journal of Wavelets, Multiresolution and Information Processing, World Scientific 16(1):1850013
10. Jindal H, Saxena S, Kasana SS (2017) Sewage water quality monitoring framework using multi-parametric sensors. Wirel Pers Commun 97(1):881–913
11. Jindal H, Saxena S, Kasana SS (2017) Triangular pyramidal topology to measure temporal and spatial variations in Shallow River water using ad-hoc sensors network. Ad Hoc and Sensor Wireless Networks, Old City Publishing 39(1–4):1–35
12. Jindal H, Saxena S, Kasana SS (2018) A sustainable multiparametric sensors network topology for river water quality monitoring. Wirel Netw 24(1):3241–3265
13. Jindal H, Saxena S, Singh S (2014). Challenges and issues in underwater acoustics sensor networks: A Review. Proceedings of International Conference on Parallel, Distributed and Grid Computing (PDGC-2014), 251–255.
14. Jindal H, Singh H, Bharti M (2018). Modified cuckoo search for resource allocation on social internet of things, in: proceedings of international conference on parallel, distributed and grid computing (PDGC-2018), 12 Solan, India
15. Kaur S, Jindal H (2017) Enhanced Image Watermarking Technique using Wavelets and Interpolation. International Journal of Image, Graphics and Signal Processing (IJIGSP) 9(7):23–35
16. Kim C, Shin D, Leng L, Yang CN (2018) Lossless data hiding for absolute moment block truncation coding using histogram modification. J Real-Time Image Proc 14(1):101–114
17. Kim C, Shin D, Leng L et al (2018) Separable reversible data hiding in encrypted halftone image. Displays 55(DEC.):71–79
18. Koohpayeh AT, Abd MA, Kohpayeh AS (2018) A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. Expert Syst Appl 112:208–228
19. Leng L, Li M, Kim C, Bi X (2017) Dual-source discrimination power analysis for multi-instance contactless palmprint recognition. Multimed Tools Appl 76(1):333–354
20. Leng L, Zhang J, Khan MK et al (2010) Dynamic weighted discrimination power analysis: a novel approach for face and palmprint recognition in DCT domain. International journal of physical sciences 5(17):2543–2554
21. Leng L, Zhang J, Xu J, et al. (2010). Dynamic weighted discrimination power analysis in DCT domain for face and palmprint recognition, 2010 International Conference on Information and Communication Technology Convergence (ICTC). 467–471

22. Liu S, Rho S, Jifara W, et al. (2018). A hybrid framework of data hiding and encryption in H.264/SVC. Discrete Applied Mathematics, 241 48–57
23. Makbol NM, Khoo BE, Rassem TH, Loukhaoukha K (2017) A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. Inf Sci 417:381–400
24. Mander K, Jindal H (2017) An Improved Image Compression Decompression Technique using Block Truncation and Wavelets. International Journal of Image, Graphics and Signal Processing (IJIGSP) 9(8):17–29
25. Mehta S, Mangat K, Jindal H (2015) Procreation of hierarchical routing using AODV. International Journal of Engineering Research in Computer Science and Engineering 2(8):47–50
26. Mittal A, Jindal H (2017) Novelty in Image Reconstruction using DWT and CLAHE. International Journal of Image, Graphics and Signal Processing (IJIGSP) 5(9):28–34
27. Mourya G, Jindal H, Saxena S (2015). Software perspective to underwater acoustic sensors network. Proceedings of International Conference on Next Generation Computing Technologies (NGCT-2015), 187–191.
28. Ouyang J, Coatrieux G, Chen B, Shu H (2015) Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping. Comput Electr Eng 46:419–432
29. Pradhan C, Rath S, Bisoi AK (2012) Non blind digital watermarking technique using DWT and cross chaos. Procedia Technology 6:897–904
30. Rasti P, Samiei S, Agoyi M, Escalera S, Anbarjafari G (2016) Robust non-blind color video watermarking using QR decomposition and entropy analysis. J Vis Commun Image Represent 38:838–847
31. Sahu N, Sur A (2017) SIFT based video watermarking resistant to temporal scaling. J Vis Commun Image Represent 45:49–64
32. Saxena S, Mehta D, Kaur J, Jindal H (2014). Acoustic Communication Characteristics in UWDBCSN. Proceedings of International Conference on Parallel, Distributed and Grid Computing (PDGC-2014), 176–180.
33. Song W, Hou J, Li Z, Huang L (2011) Chaotic system and QR factorization based robust digital image watermarking algorithm. J Cent S Univ Technol 18(1):116–124
34. Su Q (2016) Novel blind colour image watermarking technique using Hessenberg decomposition. IET Image Process 10(11):817–829
35. Su Q, Chen B (2017) A novel blind color image watermarking using upper Hessenberg matrix. AEU Int J Electron Commun 78:64–71
36. Su Q, Liu D, Yuan Z, Wang G, Zhang X, Chen B, Yao T (2019) New rapid and robust color image watermarking technique in spatial domain. IEEE Access 7(3):30398–30409
37. Su Q, Niu Y, Wang G, Jia S, Yue J (2014) Color image blind watermarking scheme based on QR decomposition. Signal Process 94(1):219–235
38. Su Q, Wang G, Jia S, Zhang X, Liu Q, Liu X (2015) Embedding color image watermark in color image based on two-level DCT. SIViP 9(5):991–1007
39. Su Q, Yuan Z, Liu D (2019) An approximate Schur decomposition-based spatial domain color image watermarking method. IEEE Access 7(1):4358–4370
40. Tang M, Song W, Chen X, Hu J (2015) An image information hiding using adaptation and radix. Optik - International Journal for Light and Electron Optics 126(23):4136–4141
41. University of Granada, Computer Vision Group n.d.. CVG-UGR Image Database, http://decsai.ugr.es/cvg/dbimagenes/c512.php.
42. University of Southern California, Signal and Inage Processing Institute n.d.. USC-SIPI Image Database, http://sipi.usc.edu/database/.
43. Yuan Z, Liu D, Zhang X, et al. (2020). New image blind watermarking method based on two-dimensional discrete cosine transform. Optik, 204

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.